



ESET

Krpanje varnostnih lukenj

..VARNOSTNI POPRAVKI ZA OPERACIJSKE SISTEME IN DRUGO PROGRAMSKO OPREMO SO POSTALI NEKAJ POVSEM OBIČAJNEGA. RAZVIJALCE PROGRAMSKE OPREME LAHKO O RANLJIVOSTI NJIHOVEGA PROGRAMJA OBVESTIJO ZVESTI UPORABNIKI, LAHKO PA TAKŠNE RANLJIVOSTI IZKORIŠČAJO NEPRIDIPRAVI..

eset NOD32 TOP 10 <small>www.eset.si</small>	
Deset najbolj razširjenih groženj v zadnjem tednu	
	število okuženih e-sporočil
Win32/Netsky.Q worm	8470
različica Win32/Injector.BZ trojan	5563
Win32/Zafi.B worm	3973
Win32/Netsky.AB worm	2067
različica Win32/Kryptik.AKX trojan	1061
Win32/Netsky.C worm	1004
Win32/MyDoom.Q worm	521
različica Win32/Kryptik.AJC trojan	213
Win32/Bagle.HE worm	190
Win32/AutoRun.TT worm	169

Vsi podatki, ki jih beležijo razvijalci protivirusnih rešitev, kažejo, da se število napadov, ki izkoriščajo varnostne luknje operacijskih sistemov, manjša, v vzponu pa so napadi, ki izkoriščajo ranljivosti v ostali programski opremi. Pisci škodljive kode so v zadnjih mesecih najpogosteje izkoriščali varnostne luknje v programih Adobe Acrobat Reader, Adobe Flash Player, Sun Java, Apple QuickTime in Microsoft Office. Dejstvo je tudi, da razvijalci operacijskih sistemov v povprečju svoje varnostne luknje s popravki zakrpajo dvakrat hitreje kot razvijalci ostale programske opreme.

Najnovejša verzija ESET Smart Security in ESET NOD32 Antivirus vključuje tudi opozorilni

sistem, ki uporabnika v primeru, da so za njegov operacijski sistem že na voljo novi varnostni popravki, na to opozarja. Ta sistem je možno kadar koli izklopiti, kar pa seveda ni priporočljivo. Zadnji večji napad, ki izkorišča varnostne luknje v operacijskih sistemih Windows, je izbruhnil novembra lani, gre pa za črv Conficker. Čeprav je Microsoft varnostno luknjo, ki jo črv izrablja, zakrpal zelo hitro, ogromno število uporabnikov svojega operacijskega sistema do danes še vedno ni posodobilo. Zato niti ne preseneča dejstvo, da Conficker še vedno vztraja na prvem mestu med vsemi zaznanimi grožnjami.

Napadalci svojo škodljivo kodo na računalnike uporabnikov skozi varnostne luknje v programski opremi najraje širijo s pomočjo e-pošte, vse bolj pa so pogosti tudi napadi na spletne strani.

Nepripravljene upravitelje spletnih strani najpogosteje presenetijo napadi, ki uporabljajo tehniko SQL injection. Ta izkorišča slabo zavarovane podatkovne baze spletnih aplikacij. Pogosto je tudi izkoriščanje ranljivosti spletnih aplikacij s Cross-Site Scripting (XSS), ki napadalcem omogoča vnašanje škodljive kode na povsem običajne spletne strani. Nič nenavadnega pa niso niti prevare kot je pred nekaj dnevi do-



letela medijskega giganta New York Times. Napadalci so se jim predstavili kot telefonsko podjetje, ki bi rado na njihovo spletno stran postavilo svoj oglas. Ta oglas so napadalci po nekaj dneh zamenjali s škodljivo kodo, ki je obiskovalce z odpiranjem nadležnih pojavnih oken napeljeval k nakupu lažnega protivirusnega programa. Veliko obiskovalcev takšnim spletnim stranem brezpogojno zaupa, zato veliko uporabnikov takšnim prevaram tudi nasede. Obstajajo pa tudi okužene strani, ki od obiskovalca prenašanja datotek z zlonamerno kodo sploh ne zahtevajo, za okužbo je dovolj že preprost obisk takšne strani.

Prepričajte se torej, da je vaš operacijski sistem ter programska oprema vedno posodobljena, pri brskanju po spletu pa uporabljajte zadnje verzije spletnih brskalnikov. Predvsem pa se prepričajte, da vaša protivirusna rešitev uporablja dobro proaktivno zaščito in zadnje zbirke virusnih definicij.

(P.R.)

NOVE GENE, PRILAGOJENE RECESIJI

Varujemo vašo zasebnost

ESET SMART SECURITY

- Antivirus
- Antispyware
- Firewall
- Antispam

ESET NOD32 ANTIVIRUS

- Antivirus
- Antispyware

www.eset.si

SI SPLET, d. o. o. | Dolenjska c. 138, Ljubljana
01 428 94 05 | info@sisplet.com

SI SPLET
INFORMACIJSKE TEHNOLOGIJE